

Inclusion-maximal integral point sets over finite fields

MICHAEL KIERMAIER* and SASCHA KURZ†
 Department of Mathematics, University of Bayreuth
 D-95440 Bayreuth, Germany

April 8, 2008

Keywords: integral distances, exhaustive search, finite geometry, Paley graphs
 MSC: 51E2, 05B25

Abstract

We consider integral point sets in affine planes over finite fields. Here an integral point set is a set of points in \mathbb{F}_q^2 where the formally defined Euclidean distance of every pair of points is an element of \mathbb{F}_q . From another point of view we consider point sets over \mathbb{F}_q^2 with few and prescribed directions. So this is related to Rédei's work. Another motivation comes from the field of ordinary integral point sets in Euclidean spaces \mathbb{E}^m .

In this article we study the spectrum of integral point sets over \mathbb{F}_q which are maximal with respect to inclusion. We give some theoretical results, constructions, conjectures, and some numerical data.

1 Introduction

The study of geometrical objects with integral edge lengths has been attractive for mathematicians for ages. The first result may be obtained by the Pythagoreans considering boxes with integral side and diagonal length. A slight generalization of this problem is even unsolved up to our times. Is there a perfect perfect box? This is a rectangular parallelepiped with all edges, face diagonals and space diagonals of integer lengths [10, 14]. In a more general context one is interested in the study of integral point sets, see [11, 20, 21] for an overview. As originally introduced integral point sets are sets of n points in the m -dimensional Euclidean space \mathbb{E}^m with pairwise integral distances. Here the most results are known for dimension $m = 2$, see i.e. [11, 12, 17, 20, 21, 26]. Although integral point sets were studied for a long time our knowledge is still very limited.

So Stanko Dimiev [9] came up with the idea of studying integral point sets over finite rings with the hope that the situation in the finite case is easier and that some structure of the problem may be preserved. So for a commutative ring \mathcal{R} with 1 we

*michael.kiermaier@uni-bayreuth.de
 †sascha.kurz@uni-bayreuth.de

consider point sets \mathcal{P} over \mathcal{R}^2 . For two points $u = (u_1, u_2)$, $v = (v_1, v_2)$ in \mathcal{R}^2 we define the squared distance as $d^2(u, v) := N(u-v) := (u_1-v_1)^2 + (u_2-v_2)^2 \in \mathcal{R}$. We say that two points u, v are at integral distance if there is an element $r \in \mathcal{R}$ with $d^2(u, v) = r^2$, meaning that the distance is an element of \mathcal{R} . Here an integral point set is a set of points in \mathcal{R}^2 with pairwise integral distances. For residue rings $\mathcal{R} = \mathbb{Z}_n$ first results were obtained in [9, 15].

If the ring \mathcal{R} is a finite field we clearly have a bit more algebraic tools at hand to attack the problem in this special case. So in [18] one of the authors studied integral point sets over \mathbb{F}_q^2 and classified those integral point sets with maximal cardinality up to isomorphism almost completely, see Section 3 for the definition of isomorphic integral point sets. To state the classification result we need some notation. For an odd prime power q there are exactly $\frac{q+1}{2}$ squares in \mathbb{F}_q . The set of squares will be denoted by \square_q . We have $-1 \in \square_q$ if and only if $q \equiv 1 \pmod{4}$. In this case ω_q will denote a fixed element with $\omega_q^2 = -1$. With this we can state:

Theorem 1 (Kurz, 2007 [18])

Let $q = p^r$ be a prime power. If $2|q$ then \mathbb{F}_q^2 is an integral point set otherwise the maximal cardinality of an integral point set \mathcal{P} over \mathbb{F}_q^2 is given by q . If $q \equiv 3 \pmod{4}$ then each integral point set of this maximal cardinality is isomorphic to $(1, 0) \cdot \mathbb{F}_q$. If $q = p \equiv 1 \pmod{4}$ then each integral point set of this maximal cardinality is isomorphic $(1, 0) \cdot \mathbb{F}_q$, $(1, \omega_q) \cdot \mathbb{F}_q$, or $(1, \omega_q) \cdot \square_q \cup (1, -\omega_q) \cdot \square_q$.

The key ingredient for this result was a theorem on point sets over \mathbb{F}_q^2 with few directions. Here two points (x_1, y_1) , (x_2, y_2) have the direction $\frac{y_1-y_2}{x_1-x_2} \in \mathbb{F}_q \cup \{\infty\}$.

Theorem 2 (Ball, Blokhuis, Brouwer, Storme, Szőnyi, 1999 [6]; Ball 2003 [4])

Let $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$, where $q = p^n$, p prime, $f(0) = 0$. Let $N = |D_f|$, where D_f is the set of directions determined by the function f . Let e (with $0 \leq e \leq n$) be the largest integer such that each line with slope in D_f meets the graph of f in a multiple of p^e points. Then we have the following:

- (1) $e = 0$ and $\frac{q+3}{2} \leq N \leq q + 1$,
- (2) $p^e > 2$, $e|n$, and $\frac{q}{p^e} + 1 \leq N \leq \frac{q-1}{p^e-1}$,
- (3) $e = n$ and $N = 1$.

Moreover, if $p^e > 2$, then f is a linear map on \mathbb{F}_q viewed as a vector space over \mathbb{F}_{p^e} . If $e = 0$ and $N = \frac{q+3}{2}$ then f is affinely equivalent to $f(x) = x^{\frac{q-1}{2}}$. (All possibilities for N can be determined in principle.)

In [2] the Bulgarian group around Dimiev considered integral point sets over \mathbb{F}_p^2 for $p \equiv 3 \pmod{4}$ which are maximal with respect to inclusion. They classified the maximal integral point sets up to isomorphism for $p = 7, 11$ and conjectured that the maximal integral point sets have either cardinality $\frac{p+3}{2}$ or p . In the latter case all p points are on a line. Theorem 1 clears the situation for cardinality p . In this article we disprove their conjecture about the spectrum of possible cardinalities of maximal integral point sets and classify them for $q \leq 47$.

2 The graph of integral distances

It turns out that it is usefull to model integral points sets as cliques of certain graphs.

Definition 1 For a fixed prime power $q = p^r$ we define the graph \mathfrak{G} with vertex set \mathbb{F}_q^2 , where two vertices v and w are adjacent if $d(v, w) \in \square_q$. So two different vertices are connected by an edge exactly if they are at integral distance. The graph \mathfrak{G} will be called graph of integral distances.

Furthermore, we recall that for $q \equiv 1 \pmod{4}$ the Paley-graph $\text{Paley}(q)$ is defined as the graph with vertex set \mathbb{F}_q where two vertices v and w are adjacent if $v - w \in \square_q \setminus \{0\}$.

2.1 The case $q \equiv 3 \pmod{4}$

Theorem 3 For $q \equiv 3 \pmod{4}$ it holds: $\mathfrak{G} \cong \text{Paley}(q^2)$.

PROOF. We define the two sets

$$M := \{(x, y) \in \mathbb{F}_q^2 \mid x^2 + y^2 \in \square_q\} \quad \text{and} \quad N := \{(x, y) \in \mathbb{F}_q^2 \mid x + yi \in \square_{q^2}\}$$

Obviously, $|N| = |\square_{q^2}| = \frac{q^2+1}{2}$, and by Lemma 1: $|M| = |P_0| + \frac{q-1}{2}|P_1| = |N|$. Let $(x, y) \in N$. Then there exist $a, b \in \mathbb{F}_q$ with $(a + bi)^2 = x + yi$. That implies $x = a^2 - b^2$ and $y = 2ab$, and we get $x^2 + y^2 = (a^2 + b^2)^2 \in \square_q$. Hence $(x, y) \in M$. Because of the finiteness of M and N we get $M = N$ and the proof is complete. \square

Now we can apply the existing theory for the Paley-graphs on our situation. For example, \mathfrak{G} is a strongly regular graph with parameters

$$(v, k, \lambda, \mu) = \left(q^2, \frac{q^2 - 1}{2}, \frac{q^2 - 1}{4} - 1, \frac{q^2 - 1}{4} \right)$$

In [5] Aart Blokhuis determined the structure of cliques of maximal size in Paley graphs of square order: A clique of maximal size of \mathfrak{G} is an affine line in \mathbb{F}_q^2 . This implies that the size of a maximal integral point set in \mathbb{F}_q is q , and—anticipating the definitions of the next section—these point sets are unique up to isomorphism.

Maximal cliques of size $\frac{q+1}{2}$ and $\frac{q-1}{2}$ in Paley graphs of square order can be found in [3].

2.2 The case $q \equiv 1 \pmod{4}$

Theorem 4 For $q \equiv 1 \pmod{4}$, \mathfrak{G} is a strongly regular graph with parameters

$$(v, k, \lambda, \mu) = \left(q^2, \frac{(q-1)(q+3)}{2}, \frac{(q+1)(q+3)}{4} - 3, \frac{(q+1)(q+3)}{4} \right)$$

PROOF. The graph consists of q^2 vertices of degree $\frac{(q-1)(q+3)}{2}$ (there are $\frac{q+3}{2}$ integral directions and $q - 1$ further points of one direction). We consider two points u and v which are at a non-integral distance. From each point there are $\frac{q+3}{2}$ integral directions. Since the direction from u to v is non-integral and non-parallel lines intersect in exactly one point we have $\mu = \frac{q+3}{2} \cdot \frac{q+1}{2}$. For the determination of λ we consider two points u and v at integral distance. Thus the direction from u to v is integral and all points on this line have integral distances to u and v . There are $\frac{q+1}{2}$ further integral directions from u and from v respectively. Each pair intersects, if not parallel, in exactly one point. By a short calculation we can verify the stated value for λ . \square

We remark that the parameters of the complementary graph of \mathfrak{G} are

$$(v, k, \lambda, \mu) = \left(q^2, \frac{(q-1)^2}{2}, \frac{(q-1)(q-3)}{4} + 1, \frac{(q-1)(q-3)}{4} \right).$$

In both cases \mathfrak{G} corresponds to an orthogonal array. We have $\mathfrak{G} \in \text{OA}\left(q, \frac{q+1}{2}\right)$ for $q \equiv 3 \pmod{4}$ and $\mathfrak{G} \in \text{OA}\left(q, \frac{q+3}{2}\right)$.

3 Automorphism group

It will be convenient to identify the affine plane \mathbb{F}_q^2 with the ring $\mathbb{F}_q[i]$ where i is a root of the polynomial $X^2 + 1 \in \mathbb{F}_q[X]$. With this identification, the map $N : (\mathbb{F}_q[i], \cdot) \rightarrow (\mathbb{F}_q, \cdot)$ is a monoid homomorphism. In the case $q \equiv 3 \pmod{4}$ we have $-1 \notin \square_q$, so $X^2 + 1$ is irreducible and $\mathbb{F}_q[i] \cong \mathbb{F}_{q^2}$. For $q \equiv 1 \pmod{4}$, \mathbb{F}_q is a finite ring with two nontrivial ideals, namely $\mathbb{F}_q(\omega_q + i)$ and $\mathbb{F}_q(\omega_q - i)$. These ideals are of order q and contain the zero-divisors of $\mathbb{F}_q[i]$. An element $z = x + iy \in \mathbb{F}_q[i]$ is a zero-divisor iff $N(z) = 0$.

In the introduction we announced that we want to classify maximal integral point sets up to isomorphism. So we have to specify what we consider as an automorphism. Now we say that an automorphism of \mathbb{F}_q^2 is a bijection $\tau : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$ with $d(x, y) \in \square_q \Leftrightarrow d(\tau(x), \tau(y)) \in \square_q$ for every $x, y \in \mathbb{F}_q^2$. This is exactly the automorphism group G of the corresponding graph \mathfrak{G} of integral distances. For Paley graphs of square order the automorphism group was known since a while, see [8, 13, 27]. If we also request that automorphisms τ map lines to lines, then the automorphism group of \mathbb{F}_q^2 for $2 \nmid q$ was determined in [18].

Theorem 5 (Kurz, 2007 [18])

Let $q = p^r \neq 5, 9$ an odd prime power, G the automorphism group of \mathbb{F}_q^2 and $H := G \cap \text{AGL}(2, \mathbb{F}_q)$. Then H is generated by

1. $x \mapsto x + v$ for all $v \in \mathbb{F}_q^2$
2. $x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot x$,
3. $x \mapsto \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \cdot x$ for all $\{a, b\} \subseteq \mathbb{F}_q^2$ such that $a^2 + b^2$ is a square, and
4. $(a, b) \mapsto (a^{p^i}, b^{p^i})$ for $i \in \mathbb{N}$.

In the next section we will describe an algorithm which calculates maximal integral point sets up to isomorphism. In order to make this algorithm really fast we want to demand weaker conditions on automorphisms as in [18] and not use the multiplication in $\mathbb{F}_q[i]$ or that lines must be mapped onto lines. Strictly speaking we choose the automorphism group G of the corresponding graph \mathfrak{G} of integral distances instead of H . It will turn out that a distinction between these two slightly different definitions of automorphisms is not necessary since we have $G \simeq H$ in many cases.

Definition 2 A triple (a, b, c) is called Pythagorean triple over \mathbb{F}_q if $a^2 + b^2 = c^2$.

In the following it will be useful to have a parametric representation of the Pythagorean triples over \mathbb{F}_q .

Lemma 1 For $2 \nmid q$ let $c \in \mathbb{F}_q$ and P_c the set of Pythagorean triples (a, b, c) over \mathbb{F}_q .

(a) Case $c = 0$

$$P_0 = \begin{cases} \{(t, \pm t\omega_q, 0) \mid t \in \mathbb{F}_q\} & \text{if } q \equiv 1 \pmod{4} \\ \{(0, 0, 0)\} & \text{if } q \equiv 3 \pmod{4} \end{cases}$$

$$|P_0| = \begin{cases} 2q - 1 & \text{if } q \equiv 1 \pmod{4} \\ 1 & \text{if } q \equiv 3 \pmod{4} \end{cases}$$

(b) Case $c \neq 0$

$$P_c = \{(\pm c, 0, c)\} \cup \left\{ \left(\frac{t^2 - 1}{t^2 + 1} \cdot c, \frac{2t}{t^2 + 1} \cdot c, c \right) \mid t \in \mathbb{F}_q^*, t^2 \neq 1 \right\}$$

$$|P_c| = \begin{cases} q - 1 & \text{if } q \equiv 1 \pmod{4} \\ q + 1 & \text{if } q \equiv 3 \pmod{4} \end{cases}$$

(c) There are exactly q^2 Pythagorean Triples over \mathbb{F}_q .

PROOF. Part (a) is easy to verify. For part (b) there are 4 solutions with $ab = 0$, these are $\{(0, \pm c, c), (\pm c, 0, c)\}$. For $ab \neq 0$ we get:

$$a^2 + b^2 = c^2 \Leftrightarrow \frac{c-a}{b} \cdot \frac{c+a}{b} = 1.$$

Setting $t := \frac{c+a}{b} \in \mathbb{F}_q^*$, we obtain

$$\frac{a}{b} = \frac{t - t^{-1}}{2} \quad \text{and} \quad \frac{c}{b} = \frac{t + t^{-1}}{2}$$

Because of $a \neq 0, c \neq 0$ we have $t^2 \notin \{-1, 1\}$. It follows

$$a = \frac{t - t^{-1}}{t + t^{-1}} \cdot c \quad \text{and} \quad b = \frac{2}{t + t^{-1}} \cdot c$$

It is easily checked that for all admissible values of t , the resulting triples (a, b, c) are pairwise different Pythagorean triples.

The expression for the number of solutions follows because -1 is a square in \mathbb{F}_q exactly if $q \equiv 1 \pmod{4}$.

With part (a) and part (b) we get the number of Pythagorean triples over \mathbb{F}_q as

$$\sum_{c \in \mathbb{F}_q} |P_c| = |P_0| + (q-1)|P_1| = q^2$$

So also part (c) is shown. \square

With the help of Lemma 1 we can easily deduce for $q \neq 5, 9$,

$$|H| = \begin{cases} q^2(q-1)^2r & \text{if } q \equiv 1 \pmod{4}, \\ q^2(q-1)(q+1)r & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

For $q = 5$ we have $|H| = 800$ and for $q = 9$ we have $|H| = 31104$. It is not difficult to prove $G \simeq H$ for $q = p \neq 5, 9$ being a prime. But since we need the automorphism

groups only for small q we simply have utilized `nauty` [22] for $q \leq 167$. We have obtained $|G| = 28800$ for $q = 5$, $|G| = 186624$ for $q = 9$, and

$$|G| = \begin{cases} q^2(q-1)^2r^2 & \text{if } q \equiv 1 \pmod{4}, \\ q^2(q-1)(q+1)r^2 & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

for the remaining cases with $q \leq 167$.

From Theorem 5 we can deduce:

Corollary 1 *For two points $p_1 \neq p_2 \in \mathbb{F}_q'$ at integral distance there exists an automorphism φ with either $\varphi(p_1) = 0$, $\varphi(p_2) = 1$ or $\varphi(p_1) = 0$, $\varphi(p_2) = 1 + \omega_q x$.*

4 Inclusion-maximal integral point sets over \mathbb{F}_q^2

For the classification of inclusion-maximal integral point sets over \mathbb{F}_q^2 we can use Corollary 1 to prescribe the point $(0, 0)$. Now we build up a graph \mathcal{G}_q which consists of the elements of \mathbb{F}_q^2 which are at integral distance to $(0, 0)$. Between two nodes $x, y \in \mathbb{F}_q^2$ there is an edge if and only if $d(x, y) \in \square_q$. For practical purposes the generation of all $\frac{q^2-1}{2}$ points which are at integral distance to $(0, 0)$ can be easily done by a for loop, as in [2]. For theoretic applications one can deduce a parametric solution from Lemma 1. The cliques of \mathcal{G}_q are in bijection to the inclusion-maximal integral point sets over \mathbb{F}_q^2 . Thus we may use a clique search program, f.e. `cliquer` [23], to search for inclusion-maximal integral point sets.

For the classification up to isomorphism we use an orderly algorithm in combination with `nauty` [22] as described in [25] on the graph \mathcal{G}_q . To guarantee that this approach yields the correct classification we have to ensure that the automorphism group of \mathcal{G}_q equals the automorphism group of the original problem. In our case we have simply checked this condition using `nauty`. We remark that we consider G as the automorphism group of the original problem and not $H \leq G$.

If we denote by $\mathcal{A}_{q,s}$ the number of non-isomorphic inclusion-maximal integral point sets over \mathbb{F}_q^2 we have obtained the following results with the above described algorithm. For $q \equiv 3 \pmod{4}$ we have:

| q | Σ | 3 | 5 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 19 | 23 | 25 | 27 | 31 | 43 | 47 |
|-----|----------|---|---|---|----|----|-----|-----|------|--------|--------|--------|-------|------|------|-----|----|----|----|----|----|
| 3 | 1 | 1 | | | | | | | | | | | | | | | | | | | |
| 7 | 2 | | 1 | 1 | | | | | | | | | | | | | | | | | |
| 11 | 4 | | | 3 | | | | | | | | | | | | | | | | | |
| 19 | 54 | | | | 25 | 7 | 19 | | | | | 4 | | | | | | | | | |
| 23 | 294 | | | | | 85 | 108 | 80 | 7 | 9 | | | 4 | | | | | | 1 | | |
| 27 | 645 | | | | | | 27 | 411 | 142 | 50 | 12 | | | | 2 | | | | | 1 | |
| 31 | 6005 | | | | | | | 60 | 2004 | 2734 | 933 | 199 | 26 | 46 | | | 2 | | | 1 | |
| 43 | 231890 | | | | | | | | 15 | 1748 | 54700 | 109127 | 54759 | 9785 | 1490 | 156 | 87 | 20 | | 2 | 1 |
| 47 | 805783 | | | | | | | | | 125545 | 434029 | 210725 | 28533 | 4904 | 628 | 230 | 27 | 50 | | 2 | 1 |

Conjecture 1 *For each $q \equiv 3 \pmod{4}$ there exist $l_q, r_q \in \mathbb{N}$ such that $r_q \leq \frac{q-1}{2}$, $\mathcal{A}_{q,l_q} > 0$, $\mathcal{A}_{q,r_q} > 0$, $\mathcal{A}_{q,\frac{q+3}{2}} > 0$, $\mathcal{A}_{q,q} > 0$, and $\mathcal{A}_{q,s} = 0$ for $s \notin \{l_q, \dots, r_q, \frac{q+3}{2}, q\}$.*

For $q \equiv 1 \pmod{4}$ we have:

| q | Σ | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 25 | 29 | 37 | 41 |
|-----|----------|---|------|-------|--------|-------|-------|-------|------|-----|-----|-----|----|----|----|----|----|----|----|----|----|----|----|----|
| 5 | 1 | 1 | | | | | | | | | | | | | | | | | | | | | | |
| 9 | 4 | 2 | | | | 2 | | | | | | | | | | | | | | | | | | |
| 13 | 30 | 2 | 11 | 8 | 5 | 1 | | | | | | | | | | | | | | | | | | |
| 17 | 107 | 8 | 57 | 24 | 12 | 2 | | | | | 1 | | | | | | | | | | | | | |
| 25 | 488 | 9 | 122 | 148 | 108 | 41 | 23 | 17 | 8 | 4 | 1 | 2 | | | | | | | | | 4 | | | |
| 29 | 9693 | 6 | 893 | 4264 | 2864 | 1230 | 284 | 116 | 22 | 6 | 3 | 2 | | | | | | | | | 3 | | | |
| 37 | 103604 | 1 | 314 | 17485 | 44952 | 24067 | 10645 | 4835 | 906 | 234 | 89 | 55 | 11 | 2 | 3 | 1 | | | | 1 | 3 | | | |
| 41 | 347761 | 1 | 1169 | 61940 | 149839 | 86159 | 33941 | 10854 | 2891 | 646 | 136 | 131 | 27 | 16 | 4 | 3 | 1 | 1 | | | | | | |

Conjecture 2 For each $q \equiv 1 \pmod{4}$ there exist $l_q, r_q, \in \mathbb{N}$ such that $\mathcal{A}_{q,l_q} > 0$, $\mathcal{A}_{q,r_q} > 0$, $\mathcal{A}_{q,q} > 0$, and $\mathcal{A}_{q,s} = 0$ for $s \notin \{l_q, \dots, r_q, q\}$.

So clearly the spectrum of possible cardinalities of inclusion-maximal integral point sets of \mathbb{F}_q^2 is a bit more complicated as conjectured in [2]. We would like to remark that for $q \in \{59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163\}$ the second largest inclusion-maximal integral point set has size $\frac{q+3}{2}$, which was verified using a clique search approach. Besides the maximum and the second largest cardinality of an integral point set also the minimum cardinality of a maximal integral point set is of interest. Here we remark that we have $l_q = 7$ for $q \neq 13$ and $11 \leq q \leq 47$. For $q \in \{49, 53, 59, 61, 67, 73\}$ we have $l_q = 8$, $l_{71} = 9$, and $l_{79} \in \{8, 9\}$.

Later on we will prove $l_q \geq 5$ for $q \geq 5$, see Lemma 8.

Conjecture 3 For each $w \in \mathbb{N}$ there exists a $q_w \in \mathbb{N}$ such that we have $l_q \geq w$ for $q \geq q_w$, meaning $\mathcal{A}_{q,s} = 0$ for $s < w$ and $q \geq q_w$.

From Theorem 1 we can conclude the following corollary:

Corollary 2 For $2 \mid q$ we have $\mathcal{A}_{q,q^2} = 1$ and all other numbers equal 0. For $2 \nmid q$ we have $\mathcal{A}_{q,s} = 0$ if $s > q$. Additionally we have $\mathcal{A}_{q,q} \geq 1$ if $q \equiv 3 \pmod{4}$ and $\mathcal{A}_{q,q} \geq 3$ if $q \equiv 1 \pmod{4}$.

Conjecture 4 For $q \equiv 3 \pmod{4}$ and $q \geq 7$ the second largest cardinality of an inclusion-maximal integral point set over \mathbb{F}_q^2 is $\frac{q+3}{2}$.

To have a deeper look at the second largest inclusion-maximal integral point sets we need some lemmas from [18].

Lemma 2 In $\mathbb{F}_q[i]$ the set $N^{-1}(1) = \{z \in \mathbb{F}_q[i] \mid z\bar{z} = 1\}$ is a cyclic multiplicative group.

PROOF. If $-1 \notin \square_q$ then $\mathbb{F}_q[i]$ is a field and thus C must be cyclic. For the case $-1 \in \square_q$ we utilize the bijection

$$\rho_q : \mathbb{F}_q^* \rightarrow N^{-1}(1), \quad t \mapsto \frac{1+t^2}{2t} + \omega_q \frac{1-t^2}{2t} x.$$

Now we only have to check that the mapping is a group isomorphism, namely

$$\rho_q(i \cdot j) = \rho_q(i) \cdot \rho_q(j).$$

□

Lemma 3 For $z \in \mathcal{R}'$ with $z\bar{z} = 1$ the set $\mathcal{P} = \{z^{2i} \mid i \in \mathbb{N}\}$ is an integral point set.

PROOF. With $c := a - b$ we have

$$\begin{aligned} d(z^{2a}, z^{2b}) &= (z^{2a} - z^{2b}) \cdot \overline{(z^{2a} - z^{2b})} = (z^{2c} - 1) \cdot \overline{z^{2c} - 1} \\ &= 2 - z^{2c} 2 - \overline{z^{2c}} = \underbrace{(z^c i - \overline{z^c} i)}_{\in \mathcal{R}}^2 \end{aligned}$$

□

These two lemmas allow us to do a circle construction. We choose a generator z of the cyclic group $N^{-1}(1)$ and set $\mathcal{P}_W := \{z^{2i} \mid i \in \mathbb{N}\} \cup \{0\}$. With this we have

$$|\mathcal{P}_W| = \begin{cases} \frac{q+1}{2} & \text{if } q \equiv 1 \pmod{4}, \\ \frac{q+3}{2} & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

It is easy to check that \mathcal{P}_W is an integral point set. For the order of the automorphism group we would like to mention

$$|\text{Aut}(\mathcal{P}_W)| = \begin{cases} (q-1)r & \text{if } p^r = q \equiv 1 \pmod{4}, \\ (q+1)r & \text{if } p^r = q \equiv 3 \pmod{4}. \end{cases}$$

Theorem 6 *For $q \notin \{5, 9\}$ \mathcal{P}_W is a maximal integral point set.*

PROOF. We identify the affine plane \mathbb{F}_q^2 with the field $\mathbb{F}_q[i]$. Let ζ a generator of the cyclic group $N^{-1}(1)$. Assume that there is a point $a \in \mathbb{F}_q[i] \setminus \mathcal{P}_W$ such that $\mathcal{P}_W \cup \{a\}$ is an integral point set. Then $N(a) \in \square_q$. The map $\rho : z \mapsto \zeta z^2$ is an integral automorphism. Let A the orbit of a with respect to $\langle \rho \rangle$. Then $\mathcal{P}' := \mathcal{P}_W \cup A$ is a integral point set, because $N(\zeta^{2n}a - \zeta^{2m}a) = N(a)N(\zeta^{2n} - \zeta^{2m}) \in \square_q$ and $N(\zeta^{2n}a - \zeta^{2m}) = N(a - \zeta^{2m-2n}) \in \square_q$.

Furthermore, let $\xi = u + vi \neq 1$ with $N(\xi) = 1$ and $u, v \in \mathbb{F}_q$. Because of $N(\xi) = u^2 + v^2 = 1$, we have $u \neq 1$. So $N(\xi - 1) = 2(1 - u) \neq 0$ and $\xi - 1$ is invertible. Thus $\zeta^n a = a$ is equivalent to $(\zeta^n - 1) = 0$, and we get that $|A|$ equals the multiplicative order of ζ . For $q \equiv 3 \pmod{4}$ we get $|\mathcal{P}_W \cup A| = q+2$, a contradiction to the maximum cardinality of an integral point set, see Theorem 1. In the case $q \equiv 1 \pmod{4}$ we have $|\mathcal{P}_W \cup A| = q$. We can easily check that in $\mathcal{P}_W \setminus \{0\}$ no three points are collinear. Thus with $\mathcal{P}_W \setminus \{0\}$ also $\mathcal{P}' = \mathcal{P}_W \cup A$ determines at least $\frac{q-3}{2}$ different integral directions. So for $p > 3$ we are either in case (1) or case (3) of Theorem 2. In case (1) there is a subset of $\frac{q+1}{2}$ collinear points. This is possible only for $q = 9$. For case (3) all q points are situated on a line. This is possible only for $q = 5$. For the other values $q < 11$ we check the stated result via a computer calculation.

So only the case $p = 3$ is left. Here we only have to consider case (2) of Theorem 2 and $e = 1$. So every line through two points of \mathcal{P}' meets the point set \mathcal{P}' in a multiple of $p^e = 3$ points. Let us fix a point $P \in \mathcal{P}_W \setminus \{0\}$. There are $\frac{q-3}{2}$ different lines trough P and a further point of $\mathcal{P}_W \setminus \{0\}$. For each of these lines l we have $A \cap l \leq 2$. One such line l' meets 0. Thus $A \cap l = \emptyset$. For all other lines l ($\# = \frac{q-5}{2}$) we have $A \cap l = 1$. Let $B := \{b \in \mathbb{F}_q[i] \mid N(b) = N(a)\}$. We have $|B| = q-1$. So all points of $B \setminus A$ lie on these lines l and l' . There are two points $P_1, P_2 \in A$ left which are not on these lines l or l' . Since we have that 0 is met by the line l'' through P_1 and P_2 , we have that no further point of \mathcal{P}' is situated on l'' . Thus we have the two additional integral directions $\overline{PP_1}$ and $\overline{PP_2}$. Thus there are in total at least $\frac{q+1}{2}$ integral directions determined by \mathcal{P}' , which is too much for case (2). \square

Remark 1 *For $q \in \{5, 9\}$ the set \mathcal{P}_W can be extended to an integral point set of size q .*

To describe another construction we need some further lemmas. (Most of them are already stated and proven in [18].)

Lemma 4 *An integral point set over \mathbb{F}_q^2 determines at most $\frac{q+3}{2}$ different directions if $-1 \in \square_q$ and at most $\frac{q+1}{2}$ different directions if $-1 \notin \square_q$.*

PROOF. We consider the points $p = a + bi$ at integral distance to 0. Thus there exists an element $c' \in \mathbb{F}_q$ with $a^2 + b^2 = c'^2$. In the case $a = 0$ we obtain the direction ∞ . Otherwise we set $d := \frac{b}{a}$ and $c := \frac{c'}{a}$, yielding $1 = c^2 - d^2 = (c-d)(c+d)$, where d is the direction of the point. Now we set $c + d =: t \in \mathbb{F}_q^*$ yielding $c = \frac{t+t^{-1}}{2}$, $d = \frac{t-t^{-1}}{2}$. The two values t and $-t^{-1}$ produce an equal direction. Since $t = -t^{-1} \Leftrightarrow t^2 = -1$ we get the desired bounds. \square

Definition 3 A line with slope $d = \frac{y}{x}$ is called vanishing line if $x^2 + y^2 = 0$. We call the direction d a vanishing direction. In all other cases d is called an integral direction if $1 + d^2 \in \mathbb{F}_q$ or non-integral direction if $1 + d^2 \notin \mathbb{F}_q$. The slope $d = \frac{1}{0} = \infty$ is integral.

We remark that a vanishing line can only occur for $-1 \in \mathbb{F}_q$ and in this case there are exactly two different corresponding slopes, $d = \omega_q$ and $d = -\omega_q$. A line with an integral direction forms an integral point set. Similar a line with a non-integral directions forms a non-integral point set. The vanishing lines form both integral and non-integral point sets.

It is well known that $\mathrm{PGL}(2, q)$ acts transitively on the pairs of a line l and a point p not on l . For the automorphism group of integral point sets we have a similar result.

Lemma 5 If L_i is the set of integral lines, L_n the set of non-integral lines, and L_v the set of vanishing lines in \mathbb{F}_q^2 , then the automorphism group Aut of integral point sets acts transitively on the pairs (l, p) where $l \in L$, $p \in \mathbb{F}_q^2$, $p \notin l$ for $L \in \{L_i, L_n, L_v\}$.

PROOF. We can easily check that Aut acts transitively on L_i , L_n , and L_v . Also after applying an automorphism l and p are not incident. Let $d = \frac{y}{x}$ be the slope of l . Now the multiplication by an invertible element $r \in \mathbb{F}_q^*$ or the addition of a vector $r \cdot (x, y)^T$ let l fix. These two types of automorphisms suffice to map each two points $p, p' \notin l$ onto each other. \square

Lemma 6 If $-1 \notin \mathbb{F}_q$, $2 \nmid q$ and \mathcal{P} is a non collinear integral point set over \mathbb{F}_q^2 , then each line l contains at most $\frac{q-1}{2}$ points.

PROOF. If l is a line with an integral pair of points on it, then its slope is an integral direction. Now we consider the intersections of lines with integral directions containing a point $p \notin l$, with l . \square

We remark that this lemma was already proved in [3, 7].

Lemma 7 If \mathcal{P} is a non collinear integral point set over \mathbb{F}_q^2 then every line l contains at most $\frac{q+1}{2}$ points.

PROOF. Analog to the proof of Lemma 6. \square

Now we construct another maximal integral point set \mathcal{P}_L . Therefore let us choose a non-vanishing integral line l and an arbitrary point p not on l . Let p' be the mirror point of p on l . If we draw the lines of integral directions from p we receive some intersections with l . These points together with p and p' form an integral point set \mathcal{P}_l (orthogonal directions are either both integral, both non-integral, or both vanishing). For $q \equiv 3 \pmod{4}$ we have $|\mathcal{P}_l| = \frac{q+3}{2}$ and for $q \equiv 1 \pmod{4}$ we have $|\mathcal{P}_l| = \frac{q+5}{2}$.

Theorem 7 The integral point set \mathcal{P}_L is maximal for $q \equiv 3 \pmod{4}$.

PROOF. We identify the affine plane \mathbb{F}_q^2 with the field $\mathbb{F}_q[i]$. Without loss of generality we choose the line \mathbb{F}_q and the point i not on \mathbb{F}_q , that is $\mathcal{P} = \mathbb{F}_q \cup \{\pm i\}$. For a point $P = x + iy \in \mathbb{F}_q[i] \setminus \mathbb{F}_q$, let σ_P the map $\mathbb{F}_q[i] \rightarrow \mathbb{F}_q[i]$, $z \mapsto x + yz$ and $S(P)$ the set of the $\frac{q-1}{2}$ points in \mathbb{F}_q which have integral distance to P . For all automorphisms ϕ it holds $S(\phi(P)) = \phi(S(P))$. Our strategy is to prove that $S(i) = S(P)$ and $d(i, P) \in \square_q$ only holds for $P = \pm i$.

It is easily checked that for all $P \in \mathbb{F}_q[i]$ we have $\sigma_P(\mathbb{F}_q) = \mathbb{F}_q$, $\sigma_P(i) = P$ and σ_P is an automorphism.

Now we define the set of automorphisms $A = \{\sigma_P : P \in \mathbb{F}_q[i] \setminus \mathbb{F}_q\}$ and the subset $B = \{\sigma_{(x,y)} : x \in \mathbb{F}_q, y \in \mathbb{F}_q \setminus \{0, 1\}\}$. Clearly, A is a subgroup of G and acts regularly on $\mathbb{F}_q[i] \setminus \mathbb{F}_q$, so $\sigma_P^k = \sigma_{P^k(i)}$. For $\sigma_{(x,y)} \in B$ it holds:

- $\sigma_{(x,y)}$ has exactly one fixed point Q on $\mathbb{F}_q[i]$, namely $Q = \frac{x}{1-y}$. Furthermore, $d(i, x + yi) \in \square_q \Leftrightarrow Q \in \mathbb{F}_q$.
- For each $k \in \mathbb{N}$: $\sigma_{(x,y)}^k(z) = x \frac{y^k - 1}{y - 1} + y^k z$ and in particular: $\sigma_{(x,y)}^{q-1} = \text{id}$.
- For all $z \in \mathbb{F}_q[i]$: $\sigma^k(z) - z = (y^k - 1) \left(\frac{x}{y-1} + z \right)$, so the point set $\{\sigma_{(x,y)}^k(z) : k \in \mathbb{N}\} \subseteq z + \mathbb{F}_q \cdot \left(\frac{x}{y-1} + z \right)$ is collinear.

It follows that for $\sigma \in B$ we have $\sigma^k \in B \cup \{\text{id}\}$ and that the order of each element of B divides $q - 1$.

Now we assume that $P = x + yi \neq \pm i$ is a point not in \mathcal{P} such that $S(P) = S(i)$ and $d(P, i) \in \square_q$.

(1) The case $\sigma_P \notin B$:

In this case σ_P is a translation and has no fixed point. Since $\gcd(q, q - 1) = 1$ we clearly have $S(i) \neq \sigma_P(S(i)) = S(\sigma_P(i)) = S(P)$, a contradiction.

(2) The case $\sigma_P \in B$, where the order p of σ_P is prime:

As seen above, p divides $q - 1$. The group action of $\langle \sigma_P \rangle$ on $S(i)$ partitions $S(i)$ into orbits of size p and one fixed point. Hence $p \mid -1 + |S(i)| = q - 3$, which yields $p = 2$. In B there is only one automorphism of order 2, it is $z \mapsto -z$. So $P = \sigma_P(i) = -i$, a contradiction.

(3) The case $\sigma_P \in B$, where the order k of σ_P is not prime:

Because of $\sigma_P(i) = P \neq i$ we have $k \neq 1$. Since $k \mid q - 1$ and $4 \nmid q - 1$, k has a prime factor $p \neq 2$. We set $\tau := \sigma_P^{p^{-1}k}$, which is an element of B of order p . With $Q = \tau(i)$ we have $\tau = \sigma_Q$. The points $i, P = \sigma(i)$ and $Q = \tau(i)$ are collinear, so $d(i, Q) \in \square_q$. One easily verifies $Q \notin \mathcal{P}$ and $S(Q) = S(P) = S(i)$. Now the previous case applied to $\tau = \sigma_Q$ gives a contradiction.

□

For $q \equiv 1 \pmod{4}$ the situation is a bit harder and we need the following result of Weil, see i.e. [24]:

Theorem 8 *Let $f(x)$ be a polynomial over \mathbb{F}_q of degree d without repeated factors and $N := |\{(x, y) \in \mathbb{F}_q^2 \mid y^2 = f(x)\}|$ then for $q \geq 5$ we have*

$$|N - q| \leq (d - 1)\sqrt{q}.$$

Theorem 9 *The integral point set \mathcal{P}_L is maximal for $9 < q = p^1 \equiv 1 \pmod{4}$.*

PROOF. We apply the same strategy as in the proof of Theorem 7 and adopt the notation. Nevertheless $\mathbb{F}_q[i]$ is not a field for $q \equiv 1 \pmod{4}$ we can define P, σ_P, A, B , and $\sigma_{(x,y)}$ in the same way. The three statements for $\sigma_{(x,y)} \in B$ remain valid. Also the order of each element in B divides $q - 1$. Let us again assume that $P = x + yi \neq \pm i$ is a point not in \mathcal{P} such that $S(P) = S(i)$ and $d(P, i) \in \square_q$. Since $\gcd(q, q - 1) = 1$ we conclude $\sigma_P \in B$, see the proof of Theorem 7. We have $S(i) = \{(u, 0) \mid u^2 + 1 \in \square_q\} = \{(u, 0) \mid (u - x)^2 + y^2 \in \square_q\}$ and $(0, 0), (x, 0) \in S(i) = S(P)$. Thus we have the implications $(u, 0) \in S(i) \Rightarrow (-u, 0) \in S(i)$ and $(u, 0) \in S(i) \Rightarrow (2x - u, 0) \in S(i)$. We conclude $\{j \cdot (u, 0) \mid j \in \mathbb{N}\} \subseteq S(i)$. For q being a prime this is only possible for $x = 0$.

So in the remaining cases we have $x = 0$. Thus we have $S(i) = \{(u, 0) \mid u^2 + 1 \in \square_q\} = \{(uy, 0) \mid (uy)^2 + 1 \in \square_q\}$. We remark that the equation $1 + u^2 = s^2$ has the parameter solution $s = \frac{t+t^{-1}}{2}$, $u = \frac{t^{-1}-t}{2}$ for $t \in \mathbb{F}_q^*$ since $0 \neq s - u = t$. So for all $t \in \mathbb{F}_q^*$ the term $1 + y^2 \left(\frac{t^{-1}-t}{2}\right)^2$ is a square. By multiplying with $4t^2$ we can conclude that $f(t) := 4t^2 + y^2(1 - t^2)^2$ is a square for all $t \in \mathbb{F}_q$. Thus for the N in Theorem 8 we have $N \geq 2q - 4$. So for $q \geq 25$ we have that $f(t)$ contains a repeated factor. We simply check the cases $q \leq 23$ by computer and now assume $q \geq 25$. So there exists an t with $f(t) = f'(t) = 0$ or there exist $a, b, c \in \mathbb{F}_q$ with $f(t) = b(a + t^2)^2$. We have

$$f'(t) = 8t - 4ty^2 + 4y^2t^3 = t \cdot (8 - 4y^2 + 4y^2t^2) = 0$$

in the first case. Since $f(0) = y^2 \neq 0$ we have $t^2 = 1 - \frac{2}{y^2}$. Inserting yields $f(t) = 4 - \frac{4}{y^2} = 0$ which is equivalent to $y^2 = 1$ or $y = \pm 1$. In the second case we get $b = y^2$, $a^2 = 1$, and $2(a + 1)y^2 = 4$. We conclude $a = 1$ and $y^2 = 1$. Thus $P = \pm 1$. \square

We remark that if we would choose l as a vanishing line in the construction of \mathcal{P}_L for $q \equiv 1 \pmod{4}$ then resulting integral point set could be completed to $(1, \pm \omega_q) \cdot \square_q$.

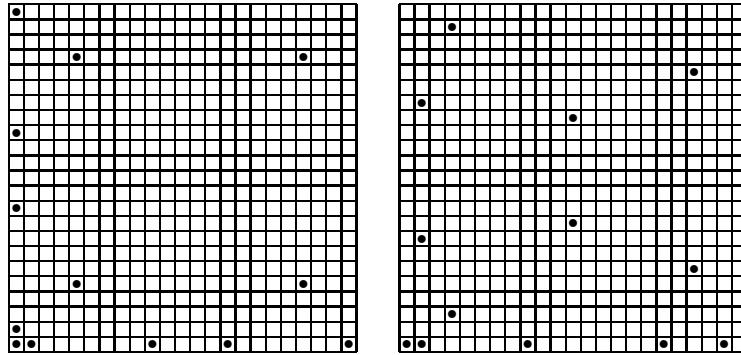


Figure 1: The integral point sets \mathcal{P}_1 and \mathcal{P}_2 .

We summarize that for $q \equiv 3 \pmod{4}$ by Theorem 6 and Theorem 7 we have two constructions showing $\mathcal{A}_{\frac{q+3}{2}, q} \geq 2$ for $q \geq 11$. One may conjecture $\mathcal{A}_{\frac{q+3}{2}, q} = 2$ for $q \geq 27$ and speak of *sporadic* solutions in the cases $q = 11, 19, 23$. The *sporadic*

solutions also have a nice geometric pattern. By z_{11} , z_{19} , and z_{23} we denote an arbitrary generator of the multiplicative group $N^{-1}(1)$ in $\mathbb{F}_{11}[i]$, $\mathbb{F}_{19}[i]$, and $\mathbb{F}_{23}[i]$, respectively. For $q = 23$ the examples are given by

$$\mathcal{P}_1 = \{0\} \cup 1 \cdot \langle z_{23}^6 \rangle \cup 3 \cdot \langle z_{23}^6 \rangle \cup 9 \cdot \langle z_{23}^6 \rangle$$

and

$$\mathcal{P}_2 = \{0\} \cup 1 \cdot \langle z_{23}^8 \rangle \cup 2 \cdot z_{23}^4 \cdot \langle z_{23}^8 \rangle \cup 6 \cdot z_{23}^4 \cdot \langle z_{23}^8 \rangle \cup 8 \cdot \langle z_{23}^8 \rangle,$$

see Figure 1. For $q = 19$ one of the two examples has a similar shape and is given by

$$\mathcal{P}_3 = \{0\} \cup 1 \cdot \langle z_{19}^4 \rangle \cup 3 \cdot \langle z_{19}^4 \rangle,$$

see Figure 2.

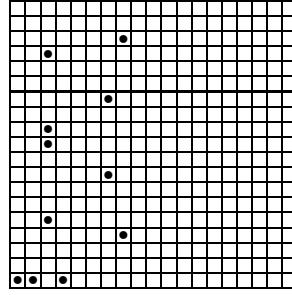


Figure 2: The integral point set \mathcal{P}_3 .

The second sporadic example \mathcal{P}_4 for $q = 19$ and the sporadic example \mathcal{P}_5 for $q = 11$ have a different geometric pattern. They are subsets of $N^{-1}(1) \cup \mathbb{F}_q \subset \mathbb{F}_q[i]$, see Figure 3.

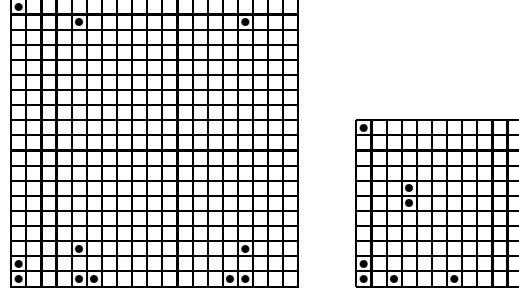


Figure 3: The integral point sets \mathcal{P}_4 and \mathcal{P}_5 .

5 Remarks on integral point sets over \mathbb{E}^2

It is interesting to mention that the situation for integral point sets in \mathbb{E}^2 is somewhat similar. Since we have an infinite of points there must not be an integral point set of

maximum cardinality. So here we ask for the minimum possible diameter $d(2, n)$ of an integral point set in the Euclidean plane \mathbb{E}^2 with pairwise integral distances, where the diameter is the largest occurring distance. Without any extra condition n points on a line would yield an integral point set with small diameter. To make it more interesting one forces integral point sets in \mathbb{E}^2 to be two dimensional. Here all known non-collinear examples of integral point sets with minimum diameter consist of a line with $n - 1$ points and one point apart, see [21, 26]. If we forbid 3 points to be collinear integral point sets on circles seem to be the examples with minimum diameter. The situation stays more or less the same if we consider integral point sets over \mathbb{Z}^2 . These results on the structure of integral point sets over \mathbb{E}^2 or \mathbb{Z}^2 are up to now only conjectures which are verified for the first few numbers n of points. So this is one motivation to study integral point sets over \mathbb{F}_q^2 in the hope that here the situation is easier to handle.

Besides the characterization of the inclusion-maximal integral point set with largest or second largest cardinality another interesting question is the characterization of those inclusion-maximal integral point sets with minimum cardinality. From our data we may conjecture that for $q \geq 11$ we have $\mathcal{A}_{q,s} = 0$ for $s \leq 6$. Again we can compare this situation to the situation in \mathbb{E}^2 . A result due to Almering [1] is the following. Given any integral triangle Δ in the plane, the set of all points x with rational distances to the three corners of Δ is dense in the plane. Later Berry generalized this results to triangles where the squared side lengths and at least one side length are rational. In \mathbb{Z}^2 the situation is a bit different. In [16] the authors search for inclusion-maximal integral triangles over \mathbb{Z}^2 . They exist but seem to be somewhat rare. There are only seven inclusion-maximal integral triangles with diameter at most 5000. The smallest possible diameter is 2066. In a forthcoming paper [19] one of the authors has extended this list, as a by-product, up to diameter 15000 with in total 126 inclusion-maximal integral triangles. So is very interesting that we have the following lemma:

Lemma 8 *If \mathcal{P} is an inclusion-maximal integral point set over \mathbb{F}_q^2 for $q \geq 5$ then we have $|\mathcal{P}| \geq 5$.*

PROOF. For small q we use our classification of maximal integral point sets over \mathbb{F}_q^2 . If $2|q$ then the only inclusion maximal integral point set over \mathbb{F}_q has size q^2 . So we assume w.l.o.g. that q is odd. Clearly an integral point set of cardinality 1 is not inclusion maximal. An integral point set \mathcal{P} of cardinality two can be completed by all other points on the line defined by \mathcal{P} . The similar statement holds for three collinear points. So let us assume that we have an inclusion maximal integral triangle $\Delta = \{p_1, p_2, p_3\}$ over \mathbb{F}_q^2 . Let l be the line through p_2 and p_3 . Starting from point p_1 there are at least $\frac{q+1}{2}$ integral directions. Lets draw lines through p_1 for these integral directions. Two of them meet p_2 and p_3 , respectively. Since at most of the remaining directions can be parallel to l we can expand Δ by least $\frac{q-5}{2} > 1$ points if $q \geq 7$. We remark that for suitable large q the cardinality $|\mathcal{P}| = 4$ may be only possible if \mathcal{P} is a point set without a collinear triple. W.o.l.g. $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ where $P_1, P_2 \in \mathbb{F}_q$ and $P_3, P_4 \notin \mathbb{F}_q$. The line through P_3 and P_4 intersects the line \mathbb{F}_q in a point $P_5 \in \mathbb{F}_q$. Since $\mathcal{P} \cup \{P_5\}$ is an integral point set and $P_5 \notin \mathcal{P}$ we have the stated result. \square

References

[1] J. H. J. Almering. Rational quadrilaterals. *Nederl. Akad. Wet., Proc., Ser. A*, 66:192–199, 1963.

- [2] A. Antonov and M. Brancheva. Algorithm for finding maximal Diophantine figures. In *Spring Conference 2007 of the Union of Bulgarian Mathematicians*, 2007.
- [3] R. Baker, G. Ebert, J. Hemmeter, and A. Woldar. Maximal cliques in the Paley graph of square order. *J. Stat. Plann. Inference*, 56(1):33–38, 1996.
- [4] S. Ball. The number of directions determined by a function over a finite field. *J. Comb. Theory, Ser. A*, 104(2):341–350, 2003.
- [5] A. Blokhuis. On subsets of $GF(q^2)$ with square differences. *Indag. Math.*, 46:369–372, 1984.
- [6] A. Blokhuis, S. Ball, A. Brouwer, L. Storme, and T. Szőnyi. On the number of slopes of the graph of a function defined on a finite field. *J. Comb. Theory, Ser. A*, 86(1):187–196, 1999.
- [7] R. Bruck. Finite nets. II: Uniqueness and imbedding. *Pac. J. Math.*, 13:421–457, 1963.
- [8] L. Carlitz. A theorem on permutations in a finite field. *Proc. Amer. Math. Soc.*, 11:456–459, 1960.
- [9] S. Dimiev. A setting for a Diophantine distance geometry. *Tensor (N.S.)*, 66(3):275–283, 2005.
- [10] R. K. Guy. *Unsolved problems in number theory. 2nd ed.* Unsolved Problems in Intuitive Mathematics. 1. New York, NY: Springer- Verlag. xvi, 285 p. , 1994.
- [11] H. Harborth. Integral distances in point sets. In *Butzer, P. L. (ed.) et al., Karl der Grosse und sein Nachwirken. 1200 Jahre Kultur und Wissenschaft in Europa. Band 2: Mathematisches Wissen. Turnhout: Brepols*, pages 213–224. 1998.
- [12] H. Harborth, A. Kemnitz, and M. Möller. An upper bound for the minimum diameter of integral point sets. *Discrete Comput. Geom.*, 9(4):427–432, 1993.
- [13] T. Khoon Lim and C. Praeger. On generalised Paley graphs and their automorphism groups. *ArXiv Mathematics math/0605252*, May 2006.
- [14] V. Klee and S. Wagon. *Old and new unsolved problems in plane geometry and number theory.* The Dolciani Mathematical Expositions. 11. Washington, DC: Mathematical Association of America. xv, 333 p. , 1991.
- [15] A. Kohnert and S. Kurz. Integral point sets over \mathbb{Z}_n^m . *Electronic Notes in Discrete Mathematics*, 27:65–66, 2006.
- [16] A. Kohnert and S. Kurz. A note on Erdős-Diophantine graphs and Diophantine carpets. *Mathematica Balkanica*, 20(3-4), 2006.
- [17] T. Kreisel and S. Kurz. There are integral heptagons, no three points on a line, no four on a circle. *submitted*, 2006.
- [18] S. Kurz. Integral point sets over finite fields. (preprint).
- [19] S. Kurz. On generating integer heronian triangles. (in preparation).

- [20] S. Kurz. *Konstruktion und Eigenschaften ganzzahliger Punktmengen*. PhD thesis, Bayreuth. Math. Schr. 76. Universität Bayreuth, 2006.
- [21] S. Kurz and A. Wassermann. On the minimum diameter of plane integral point sets. (preprint).
- [22] B. D. McKay. Practical graph isomorphism. Numerical mathematics and computing, Proc. 10th Manitoba Conf., Winnipeg/Manitoba 1980, Congr. Numerantium 30, 45-87 (1981)., 1981.
- [23] S. Niskanen and P. Östergård. Cliquer user's guide, version 1.0. Technical Report T48, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, 2003.
- [24] T. Petersen. Polynomials over finite fields whose values are squares. *Rose-Hulman Undergraduate Mathematics Journal*, 2(1):12 pp., 2001.
- [25] G. F. Royle. An orderly algorithm and some applications in finite geometry. *Discrete Math.*, 185(1-3):105–115, 1998.
- [26] J. Solymosi. Note on integral distances. *Discrete Comput. Geom.*, 30(2):337–342, 2003.
- [27] D. Surowski. Automorphism groups of certain unstable graphs. *Math. Slovaca*, 53(3):215–232, 2003.